

Appln No. 09/688,456

Amdt date March 7, 2005

Reply to Office action of December 6, 2004

**REMARKS/ARGUMENTS**

Claims 1-70 are presently pending. Claims 1 and 41 are amended.

The Examiner has not acknowledged receipt of the IDS that was filed on December 3, 2004. Applicants respectfully request acknowledgment of the IDS by initialing and returning the attached copy of the same IDS.

Claims 1-70 are rejected under 35 U.S.C. §103(b) as being unpatentable over Whitehouse, U.S. Patent 6,005,945 ("Whitehouse") over Leon, U.S. Patent 6,424,954 ("Leon"). Applicants submit that all of the claims currently pending in this application are patentably distinguishable over the cited references, and reconsideration and allowance of this application are respectfully requested.

Amended independent claim 1 includes, among other limitations, "wherein the plurality of cryptographic devices share a secret and each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users." None of the cited references, alone or in combination, disclose or teach the above limitation.

First, Whitehouse does not disclose or suggest that "the plurality of cryptographic devices share a secret." The Examiner has construed the central computer of Whitehouse as the claimed cryptographic device. Although, the central computer of Whitehouse includes "encryption keys 164 needed to generate the digital signatures in postal indicia, and keys for secure communications with the postal authority computer system 180" (col. 8, lines 38-40), the postal authority computer system can

**Appln No. 09/688,456**

**Amdt date March 7, 2005**

**Reply to Office action of December 6, 2004**

not also be construed as a cryptographic device. Rather, the postal authority computer system is used to verify the postage indicia already printed on the mail pieces. (Col. 8, line 65 to col. 9, line 11).

Similarly, Leon does not teach or suggest that "the plurality of cryptographic devices share a secret." Rather, Leon teaches a dedicated secure metering device (SMD) connected to each of the user's computers as an external hardware device or circuit card that is portable. The SMD couples to the personal computer via a communications link 122. (Col. 3, line 61 to col. 4, line 20, and FIGs. 1A and 1B.). There is no sharing of a secret between these SMD devices of Leon. In fact, by connecting a dedicated tamper proof SMD to each Users' PC, Leon teaches away from sharing a secret between the SMDs.

Second, there is no disclosure in Whitehouse that "each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users." In order to do this, the alleged central computers of Whitehouse need to be "stateless," and include the necessary software to do so. (See, for example, Specification, page 8, lines 28.). Whitehouse does not teach, nor does it suggest, such a capability.

With respect to Leon the dedicated SMDs connected to each users' computer teaches away from "the plurality of cryptographic devices shar[ing] a secret."

Third, the central computer of Whitehouse does not include a "cryptographic engine for cryptographically protecting data." As recited by claim 1. Applicants respectfully disagree with

**Appln No. 09/688,456**

**Amdt date March 7, 2005**

**Reply to Office action of December 6, 2004**

the characterization of stored encryption keys of Whitehouse as the claimed "cryptographic engine." Rather, these encryption keys are used by the CPU 150 (FIG. 4) to "generate the digital signature in postal indicia." (Col. 8, lines 38-30).

In contrast, the present invention includes "a processor programmed to authenticate a plurality of remote users" and "a cryptographic engine for cryptographically protecting data."

Accordingly, neither Whitehouse nor Leon, alone or in combination, teach or suggest the present invention, as claimed by the independent claim 1. Therefore claim 1 is patentable in view of the cited references.

Amended independent claim 41 includes, among other limitations, "creating a secret by one of the plurality of cryptographic devices," and "exporting the created secret to the remaining of the plurality of cryptographic devices to be shared among the plurality of cryptographic devices." None of the cited references, alone or in combination, disclose or teach the above limitation.

Again, as discussed above, Whitehouse does not teach or suggest creating a shared secret by one of the plurality of cryptographic devices. Furthermore, Whitehouse does not teach or suggest "exporting the created secret to the remaining of the plurality of cryptographic devices to be shared." There is no teaching in Whitehouse that the central computers export secret to each other. Moreover, Leon's dedicated SMDs do not communicate with each other and do not export secret to each other. Consequently, claim 41 is also patentable in view of the cited references.

**Appln No. 09/688,456**

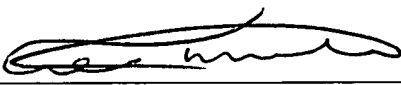
**Amdt date March 7, 2005**

**Reply to Office action of December 6, 2004**

In short, the independent claims 1 and 41 define a novel and unobvious invention over the cited references. Dependent claims 2-40, and 42-70 are dependent from claims 1 and 41, respectively and therefore include all the limitations of their respective independent claims and additional limitations therein. Accordingly, these claims are also allowable over the cited references, as being dependent from allowable independent claims and for the additional limitations they include therein.

In view of the foregoing amendments and remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance are respectfully requested.

Respectfully submitted,  
CHRISTIE, PARKER & HALE, LLP

By   
Raymond R. Tabandeh  
Reg. No. 43,945  
626/795-9900

RRT/clv  
RRT PAS611732.1-\* -03/7/05 3:28 PM